ISSN 2319 – 7595
Volume 8, No.2, March - April 2019
International Journal of Information Systems and Computer Sciences
Available Online at http://warse.org/IJISCS/static/pdf/file/ijiscs15822019.pdf
https://doi.org/10.30534/ijiscs/2019/15822019

Evaluation of Supply Chain Management based on Block Chain Technology and Homomorphism Encryption

Keerthy Prasannan[1], Bibin Varghese[2], Smita C Thomas[3]
[1]Mount Zion College of Engineering, India, 786keerthy@gmail.com
[2]Mount Zion College of Engineering, India, bibinv019@gmail.com
[3]Mount Zion College of Engineering, India, smitabejoy@gmail.com

ABSTRACT

Information sharing, analysis of various company and customer demands, planning activities etc can be coordinated and monitored with the help of supply chain management system. The planning algorithms are disturbed with the asymmetric information between companies. One of the major problem in supply chain management is double marginalization. This paper proposes a block chain based solution and homomorphism encryption to address the problems of supply chain such as double marginalization and information asymmetry etc.

Key words : Block chain, Hash function, Smart contract, Supply chain management.

1. INTRODUCTION

In a supply chain Information sharing and technology is the one of the key aspects of coordination amongst different parties. The efficiency of Supply chain is highly important because today's competition is no longer between companies, but between supply chains. Sharing of Information can increase supply chain efficiency by reducing inventories and smoothing productions.

Sharing of information can radically improve the way global companies and their partners do business, especially in the wake of increasingly globalization and outsourcing. It have a profound effect on supply chain operations. By exchanging information such as inventory levels, forecasting data, and sales trends, companies can reduce cycle times, fulfill orders more quickly, cut out millions of dollars in excess inventory, which helps to improve forecast accuracy and customer service. Manual order processing, spreadsheet dependent and fax/phone are the method of communication with suppliers in the past made a dent not only to the corporate procurement budget but also generated global operational plans that were out-of-date because of limited visibility into supplier's plan and operational constraints. Global organizations can harness the power of technology to collaborate with their supply chain partners to exchange information and work as a single entity. All this can be done with the end objective of having greater understanding of the end consumer behavior and effectively responding to the changes in the market place from a supply chain perspective. Therefore the manufacturers make the products only when they are needed and retailers store and sell them to end customers, drastically cutting down on their own inventory levels and associated costs. In the long term timely exchange of information will not improve supply chain responsiveness and it will also enhance cash flow and profitability to every link in the supply chain and helps ultimately contribute to consumer satisfaction.

Independent firms manage different parts of global supply chains when dramatic changes in manufacturing and distribution including globalization and outsourcing. Each firm in the supply chain sets strategic and operational goals to maximize its own profit. It is important to built competitive supply chain which is one of the most valuable resources for the manufacturers. ***This paper discusses the impacts of information sharing in supply chains along with the associated benefits. Challenges posed in the process of information sharing are also listed out.***

2. LITERATURE SURVEY

The principle of blockchain technology, and according to the characteristics of power demand response, the private blockchain is chosen to solve the problem of mutual trust between users, load aggregators and power grids in multi-level demand response reliable communication. Smart contracts are used to solve the problem of demand response automation in [3]. Identification of trust factor and rewarding nature of bitcoin system, and analyzes bitcoin features which may facilitate bitcoin to emerge as a universal currency is demonstrated in [2]. Paper presents the Bitcoin, one major virtual currency, attracts users' attention [1] by its novel mode in recent years. Blockchain as its basic technique, Bitcoin possesses strong security features which anonymizes user's identity to protect their private information. However, some

criminals utilize Bitcoin to do several illegal activities bringing in great security threat to the world[4]. Therefore, it is necessary to get knowledge of the current trend of Bitcoin [7] and make effort to de-anonymize in [6]. In this paper, we put forward and realize a system to analyze Bitcoin from two aspects: blockchain data and network traffic data, gap between proposed theoretical-architecture and current practical implementation of bitcoin system [5] in terms of achieving decentralization, anonymity of users, and consensus. Hash function plays an important role in the area of information security [8]. It is widely used to provide data integrity ,message authentication, digital signature and password protection. Since incremental hash function and it has gained much attention for its property. It is high-speed to compute hash value of updated message according to previous hash value instead of re-computing it from scratch as traditional hash function. it possesses not only efficiency but also security problems. have been demonstrated in [9]. In this paper, [11] the characteristics and infrastructure of the block chain is analyzed and the distributed energy trading frame work based on the block chain is built and distributed. The result shows that block chain has significant effect on the information security of the energy transaction. Block chain is a combination of a variety of technologies of the product. It develop with cryptography, mathematics, computer networks etc [12]. Architecture of a block chain includes six layers from bottom to top: data layer, network layer, consensus layer, incentive layer, contract layer, and application layer [10]. The data layer encapsulates the underlying data blocks, related data encryption, and time stamps. The network layer includes distributed networking mechanism, such as data propagation mechanism and data verification mechanism. Consensus layer mainly encapsulates the consensus algorithm of network nodes. The incentive layer integrates the economic factors into the system of block chain technology ,mainly including the economic incentive issuing mechanism and the distribution mechanism.

3. EXISTING SYSTEM

Demand forecasting is becoming difficult because of short product life cycles and long production lead times. Then,supply chains face the risk of either excess capacity due to low demand realization or lack of product availability. In a decentralized supply chain, lack of proper capacity risk sharing increases the cost of capacity risk. To deliver on time, the contract manufacturer secures capacity in advance of an original equipment manufacturer order. For such a supplychain, if consumer demand turns out to be high, both the contract manufacturer and the original equipment manufacturer face upside capacity risk. However, if consumer demand turns out to be low, only the contract manufacturer faces downside capacity risk. To reduce capacity risk for each party depends on the contractual agreements. Under a wholesale price contract, the original equipment manufacturer pays a wholesale price w to the contract manufacturer for each unit ordered and sells the product to the market at r per unit. The contract manufacturer secures capacity at a unit cost of c, which could represent an equivalent annual cost of capacity. So, the contract manufacturer's marginal profit w-c is less than the vertically integrated supply chain's marginal profit r-c. This difference is known as double marginalization. The contract manufacturer protects itself by securing less capacity than what would be optimal for a vertically integrated supply chain.

3.1 Centralized Ledger

There are multiple ledgers, but Bank holds the “golden record” Client B must reconcile its own ledger against that of Bank, and must convince Bank of the “true state” of the Bank ledger if discrepancies arise.

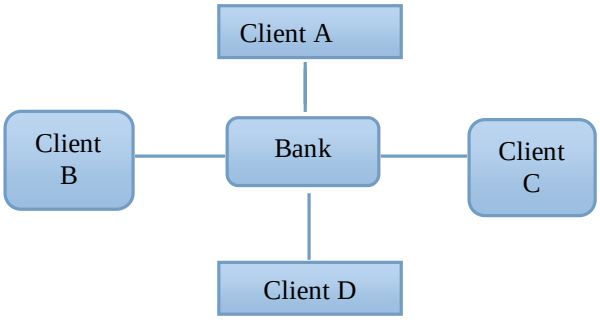


Figure 1: Centralized Ledger

3.2 Distributed Ledger

1. There is one ledger.All nodes have some level of access to that ledger.
2. All nodes agree to a protocol that determines the true state of the ledger at any point of time.
(iii) Application of this protocol is sometimes called achieving consensus.
3. It can be used without a central authority by individuals or entities with no basis to trust each other.
4. It can be used to create value or issue assets.
5. It can be used to transfer value or the ownership of assets.
6. A human being or a Smart Contract can initiate the transfer. It can be used to record those transfers of value or ownership of assets.
7. These records may be very difficult to alter, such that they are sometimes called effectively immutable.
8. It can be used to allow owners of assets to exercise certain rights associated with ownership, and to record the exercise of those rights.
9. Proxy Voting

Through observation of several industries, the unit cost of capacity and the degree of forecast information asymmetry are two primary drivers of capacity risk. There exist two types of contracts that enable credible forecast information sharing. The first contract type is a capacity reservation contract, which holds the original equipment manufacturer accountable for its forecast information by requiring a fee for reserving capacity. The contract manufacturer provides this contract as a menu of fees for corresponding capacity level that the original equipment manufacturer may reserve.

The optimal reservation price has the characteristics of a quantity discount. The second contract type is an advance purchase agreement, which provides an option to the original equipment manufacturer to place firm orders at an advance purchase price before the contract manufacturer secures capacity. This agreement credibly signals the original equipment manufacturer's forecast and induces the contract manufacturer to secure the necessary capacity. Depending on the per unit cost of capacity and the degree of forecast information asymmetry, original equipment manufacturer and contract manufacturer can choose among structured agreements that enable a mutually beneficial partnership.

3.3 Proof-Of-Work Algorithm

(i) Any given PoW is easy to verify.
(ii) The PoW is difficult to generate.
(iii) The difficulty of the PoW is parametrizable.
(iv) It should not be possible to reuse previously generated PoWs.
(v) It should not be possible to generate PoWs ahead of time and use them later.
The first three are the basic requirements for a PoW, which are also highly relevant in other application scenarios. Requirements 4 and 5 are particularly relevant in the context of cryptographic currencies, as we will demonstrate in this section. The PoW is easy to verify since any given PoW value is the result of the underlying hash function and hence can be verified by rerunning the hash function on the same input (easy to compute). The PoW is difficult to generate, i.e., only through brute force search, because it is infeasible to generate messages that correspond to a specific output of a cryptographic hash function (pre-image resistance). The difficulty of the PoW is ecause there is a range of allowed hash values that are accepted as valid PoW.

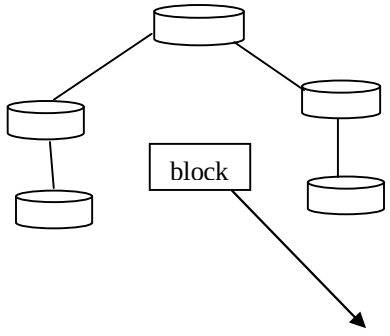
4. PROPOSED SYSTEM

Research works have discussed the benefits of information sharing throughout the supply chain. Sharing data such as machine loads, sales previsions and inventory positions has proven to improve the fulfill rate and the product cycle time, and to decrease order fluctuations. It is difficult to share information in global supply chain because there are many code schemes. The EDI network is an easy solution to integrate code schemes and realize visibility of supply chain, but it is expensive especially for small businesses.
If they try to integrate their code schemes and realize visibility of supply chain by using same ERP package such as SAP, it makes another problem. Most companies don't necessarily want to share information, because they don't want to share their capacity with competitors. Our block chain scheme has no valuable things such as virtual currency to avoid hacking. Miner can earn the transaction fee and it uses only computational power in the network. A new block chain scheme for information sharing. It brings many benefits for SCM. Users are not required to trust any third-party and are always aware of the data that is being collected about them and how it is used.

4.1.Blockchain Technology

A Blockchain is a type of diary or spreadsheet containing information about transactions. Each transaction generates a hash. A hash is a string of numbers and letters.

Transactions are entered in the order in which the occurred. Order is very important. The hash depends not only on the transaction but the previous transaction's hash. Even a small change in a transaction creates a completely new hash. The nodes check to make sure a transaction has not been changed by inspecting the hash. If a transaction is approved by a majority of the nodes then it is written into a block. Each block refers to the previous block and together make the Blockchain. A Blockchain is effective as it is spread over many computers, each of which have a copy of the Blockchain. These computers are called nodes. The Blockchain updates itself every 10 minutes.
To describe an overview of our proposed system there are two entities comprising the system. One is company which is interested in building supply chain management and another is blockchain node. The entities entrusted with maintaining the blockchain and a distributed public/private protected data store in return for incentives. Generally, information sharing scheme is exclusively tied to the major IT companies serving as the trusted third party which process and mediate any electronic transaction. The main role of the trusted third party is to validate, safeguard and preserve transactions. Certain percentage of trouble is unavoidable in online transactions and that needs mediation by transactions. This results in high transaction costs.



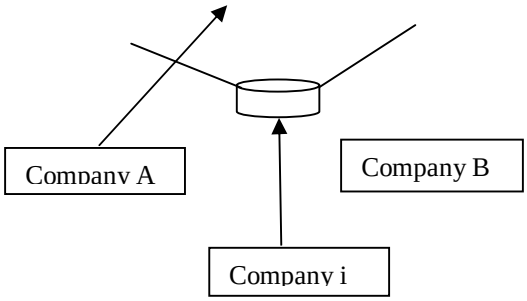


Figure 2: Transaction Process Overview

5. CONCLUSION

A new blockchain scheme for information sharing is explained in this paper. It is beneficial for supply chain management in many ways. In general, Transaction data should not be trusted in the hands of third-parties because they are susceptible to steals and misuse. To solve this problem users should own and control their data without compromising security or limiting companies' and authorities' ability to provide encrypted transactions. This is enabled by combining a blockchain with a homomorphic encryption solution. Users are not required to trust any third-party and they need to focus on their data collection and usage. The blockchain recognizes the users as the owners of their encrypted data. Companies can focus on utilizing data without being overly concerned about properly securing and compartmentalizing them. A decentralized platform, making legal and regulatory decisions about collecting, storing and sharing sensitive data is much simpler.

The laws and regulations could be programmed into the blockchain itself, so that they are enforced automatically. In some situations, the ledger can act as legal evidence for accessing (or storing) data. We recognize some problems to be solved. For example, Search operation for emergency order brings Heavy load to Miner occurs when search operation for emergency order takes place and we need to consider about efficient incentive mechanism.

ACKNOWLEDGMENT

Keerthy Prasannan thanks, first and foremost, Almighty God, without his support this work would not have been possible and all the faculty members of Mount Zion College of Engineering, for their immense support.

REFERENCES

1. Decarolis DM and Deeds DL. **The impact of stocks and flows of organizational knowledge on firm performance: an empirical investigation of the biotechnology industry, Strategic Management Journal** , Vol 4,pp.19, 275-288.S.
2. LiuFei Chen, YuShan Li, Hong Wen , WenJing Hou. **Block Chain Based Secure Scheme For Mobile Communication**, *IEEE Conference on Communications and Network Security (CNS):* IEEE CNS, 76, 145-155.
3. Gaoying Cui, Kun Shi**. Application of Block Chain in Multi - level Demand Response Reliable Mechanism,** *International Conference on Information Management.*
4. Puneet Kumar Kaushal, Dr. Amandeep Bagga and Dr. Rajeev Sobti. **Evolution of Bitcoin and Security Risk in BitcoinWallets,** *International Conference Jaipur,*
5. Yujie Xu , Mingming Wu ,Yue Lv and Shujun Zhai**. Research on Application of Block Chain in Distributed Energy Transaction,** State Grid Tianjin Power Economics &Technology Research Institute, Hedong District, Tianjin 300171.H. Poor.
6. Su Yunling**. An Overview of Incremental Hash Function Based on Pair Block Chaining**, International Forum on Information Technology and Application (2010). https://doi.org/10.1109/IFITA.2010.332
7. Jiawei Zhu, Peipeng Liu and Longtao He. **Mining Information on BitcoinNetworData** IEEE International Conference on Internet of Things (iThings) and IEEE Green .Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData).
8. S. Nakamoto**. Bitcoin: A peer-to-peer electronic cash system ,** 2010
9. E. Androulaki, G. O. Karame, M. Roeschlin and T. Scherer**. Evaluating user privacy in bitcoin**, in International Conference on Financial Cryptography and Data Security.
10. P. Koshy, D. Koshy and P. Mcdaniel. **Analysis of Anonymity in Bitcoin Using P2P Network Traffic.**
11. A. Biryukov, D. Khovratovich andI. Pustogarov**. Deanonymisationof clients in bitcoin p2p network,** Eprint Arxiv, pp. 15–29, April 2014. https://doi.org/10.1145/2660267.2660379
12. D. Ron and A. Shamir**. Quantitative Analysis of the Full Bitcoin Transaction Graph**,Springer Berlin Heidelberg, July 2013. https://doi.org/10.1007/978-3-642-39884-1_2